MANAGING VULNERABILITIES, THREATS, AND RISKS DURING THE 2020 HOLIDAY SEASON

As the business landscape continues to evolve to keep up with an increasingly remote clientele and workforce, it's a great time to revisit our discussion of IT security vulnerabilities, threats, and risks and review what financial organizations should be aware of going into the approaching holiday season, which will be a litmus test of our new normal.

IT security, and cybersecurity, in particular, has moved front and center as an ongoing concern with so much of everyday business happening across expanded endpoints and data streams and more bad actors attempting to take advantage of those new avenues. According to KPMG's recently released Pulse of Fintech study for H1 2020, the cybersecurity market so far this year has already vaulted well past all of 2019 as more companies look for ways to shore up access and establish or transform their privacy controls and fraud detection and prevention efforts. Investments in artificial intelligence and automation are also thriving.

One of the biggest shifts this holiday season, aside from moving mostly online, is that the shopping season has expanded, with Amazon's annual Prime Day, which was pushed this year to October, marking the unofficial kickoff. Many brick-and-mortar stores are closing their doors on Black Friday to discourage the crowded free-for-alls that typically mark the day.

Instead, Black Friday—which last year generated $7.4 billion in online sales—has been replaced by promotions running from now through the end of the year. That means the spike in money changing hands that used to occur within a narrow window of a few days or weeks is now spanning months.

And the touchpoints are expanding, too, with $2.9 billion of last year's Black Friday online sales happening through smart phones.

So, what's the difference between a vulnerability, a threat, and a risk?

A **vulnerability** refers to a known weakness of an asset or resource that can be exploited by one or more attackers, creating an opportunity for an attack to succeed. As an example, ransomware attacks often occur through a vulnerable access point such as weak passwords. When you're password-protecting your most sensitive data and resources, Infosecurity Group recommends checking user passwords against NCSC's top 100,000 most hacked passwords.

A **threat** is a new or newly discovered natural, unintentional, or intentional incident that has the potential to harm a system or your company. This year, that's meant everything from the extraordinary natural disasters to accidental credential security lapses created by sending your workforce home. Many now-remote employees are using company-issued devices or BYOD (bring your own device) as part of their "one life" device to access work files and shop online.

To head off potential disaster, companies should ensure that whatever device is being used for work is current on all of its security settings, patches, and updates. The pointer above about picking good passwords stands here, too. Also encourage or require VPN use for remote workers when they're accessing corporate networks.

A **risk**—loss of money, privacy, or life; reputational damage, and legal ramifications—occurs when a threat exploits a vulnerability. This is the fallout when vulnerabilities and threats are successful. An example of this would be a data breach achieved through email phishing that exposed social security numbers and private financial data. According to Security Boulevard, breaches have skyrocketed this year, with 16 billion records exposed as of August 1st, and 8.4 billion records exposed in Q1 alone, a 273 percent increase compared to the first half of 2019.

Downtime equals dollars lost, so every moment is precious, especially as we head into what could be the busiest online commerce season ever seen. Financial organizations should already have the latest authentication protocols in place for logins and email access, be conducting continuous monitoring and penetration testing, and have plans in place for data recovery, failover, and cloud backups, etc. in case an incident occurs. Automated solutions that identify, block, and report anomalous behavior are also important tools to have in the arsenal.

Companies should also ensure that staff are trained and up to date on the latest privacy and security protocols to protect both internal data and that of their customers. Empower them to spot and report intrusion attempts like the aforementioned phishing, which can expose system vulnerabilities and introduce viruses, malware, and even ransomware into the network.

Being on guard now, and planning ahead for the likelihood of a vulnerability, threat, or risk during the approaching holiday season can help keep your business on track, so it actually is the most wonderful time of the year for you, your employees, and your customers.